Commonwealth of Kentucky
Cabinet for Health and Family Services

Information Technology (IT) Policies

KENTUCKY CABINET
FOR HEALTH AND FAMILY SERVICES

020.201 Server Patch Management

Version 2.0
October 22, 2015

Revision History

Date	Version	Description	Author
9/2/2002	1.0	Effective Date	CHFS IT Policies Team Charter
10/22/2015	2.0	Revision Date	CHFS IT Policies Team Charter
10/22/2015	2.0	Review Date	CHFS IT Policies Team Charter

Table of Contents

020.201 Server Patch Management Policy

Category: 020.000 Managerial Security

1.1 Policy

Hardware and operating system patches will be applied monthly to all CHFS servers within 30 days of the patch's release. Notification will be presented to the Change Control Board (CCB) utilizing the Change Request process (see CHFS IT Policy #010.103). Emergency patches will be applied to all CHFS servers as soon as possible, but no later 7 days after receiving the patch.

All patches and hot fixes will be documented on an informational change control before being applied to the first server.

Patches will be applied in three (3) stages:

- Stage 1 – All patches will be applied to all Development environment servers on the first Thursday following their release.
- Stage 2 – All patches will be applied to all Test environment servers on the Thursday following the patching of the Development environment.
- Stage 3 – All patches will be applied to all UAT environment servers the weekend following the patching of the Test environment.
- Stage 4 – All patches will be applied to all Production environment servers the weekend following the patching of the UAT environment.

The responsible application administrator for development and test environments will arrange system down time. The move to the appropriate production environment will occur after normal business hours with the consent of the responsible application administrator. Any makeup dates will need CCB approval for any reschedule.

Emergency and Out of Band Patches:
These patches will be reviewed within 24 hours and if approved by the OATS IT Security and Audits Section, will be applied no later than the time frame for Operating System patches, identified previously.

Service Packs and/or Releases are considered upgrades to the Operating System and will be handled on a case by case basis.

1.2 Scope

This policy applies to CHFS IT employees and contractors; including all persons providing contractor services.

1.3 Definitions

- Production is defined as any server not in the Development, Test, or User Acceptance Testing/Training (UAT) environments.
- All servers are labeled (Development, Test, Production, etc) in Information Technology Management Portal (ITMP). For example, File Servers are labeled as Production.
- Any server connected to a CHFS owned network, but not managed by CHFS must follow this policy.

1.4 Policy/Procedure Maintenance Responsibility

The Office of Administrative and Technology Services (OATS) Division of Systems Management (DSM) is responsible for the maintenance of this policy.

1.5 Exceptions

Any exceptions to this policy must follow the procedures established in CHFS IT Policy #070.203.

1.6 Review Cycle

Annual

1.7 Cross References

- COT Project Framework Initiative
- COT-082 – Critical Systems Vulnerability Assessments
- CHFS IT Policy #010.103 – Change Control
- CHFS IT Policy #070.203 – Exceptions to Standards and Policies